Conveying Security Program Effectiveness

Joshua G. Kuntz CISSP (ISC)²

Information Security Officer

Texas Department of Motor Vehicles

Effective C-Level Communication

- Know your organization's business
- Build Trust with the Executive level
- Define your security program
- Develop Security Initiatives
- Articulating the effectiveness of the security program

Know Your Organization's Business

- You can't secure what you don't understand
- Define the Security mission, vision, and goals
  - Enable the business to operate securely
  - The Security Management Team sets the standard for effective and efficient security programs in the state
  - Confidentiality, Integrity, and Accessibility of the organization's data
- Security mission alignment with Organization mission

Build Trust with the Executive Level

- Don’t be the shop of NO
- Find a secure path to YES
- Understand the Trusted Advisor role
- Establish your organization’s “risk appetite”
- Have the difficult conversations about risk without ultimatums

Define Your Security Program

- Model your security program against a standard
  - Texas Cybersecurity Framework
  - NIST 800.53, ISO 27001
- Identify the compliance regulations governing your organization
  - CJIS, PCI, HIPPA, FTI, etc
- Measure your security program and identify gaps

Develop Security Initiatives

- Identify areas of low maturity
- Prioritize efforts to maximize effectiveness
- Look for “quick wins” or “low hanging fruit”
- Tie your funding requests to increasing the security posture to support organizational objectives

Articulating the Effectiveness of the Security Program

- Explain the inherent ROI problem of a Security Program
- Start with recent accomplishments
- List Audits and Audit Follow Up
- Demonstrate additional participation in the security community
- Discuss Resiliency Planning

- Develop Effectiveness Measures
  - Event to Incident Ratios
    - Email Spam & Malware
    - Web Blocks
    - Network Events
  - Volume of work over time
  - Average time to resolve incidents
    - Cost of incident resolution

Final Thoughts

- Know the business
- Establish trust with Executives
- Understand the Trusted Advisor Role
- Define your Security Program
- Develop Security Initiatives
- Articulate Security Program Effectiveness

Contact Information

Joshua G. Kuntz CISSP$_{(ISC)^2}$

joshua.Kuntz@txdmv.gov